"Express Mail" mailing label number:

EV 335895705 US

A SYSTEM AND METHOD FOR ACCESSING NETWORK AND DATA SERVICES

David Patron
Michael Grannan
Bach Hoang
Sreenivasa Gorti

FIELD OF THE DISCLOSURE

[0001] The present disclosure relates to communication networks, and more particularly to a system and method for accessing network and data services.

BACKGROUND OF THE DISCLOSURE

[0002] In recent years, wireless local area networks have become more pervasive. Some of these networks have an ad-hoc or peer-to-peer schema, while others employ a hub-based schema. Ad-hoc wireless networks usually consist of several computing devices, each equipped with a wireless transceiver. The individual devices communicate directly with one another wirelessly. Ad-hoc networks may be employed to share files or printers. In many circumstance, the computing devices of an ad-hoc wireless network will not be able to access wired local area network (LAN) resources unless one of the devices acts as a bridge to the wired LAN.

[0003] Wireless networks designed to utilize a hub-based schema often have an access point acting as the hub and providing a central point of connectivity for the wireless computing devices that make up the wireless LAN. In addition to acting as a central point of connectivity for the network, the hub may connect or "bridge" the wireless LAN to a wired network, allowing "connected" wireless computing devices to access LAN resources as well as broader network resources.

[0004] One popular incarnation of wireless networking technology involves the wireless-Ethernet standard known as IEEE 802.11. Of the various 802.11 compliant solutions, Wi-Fi may be the most popular. Wi-Fi (which may be implemented as "802.11b", "802.11g" and/or "802.11a") has emerged as a dominant standard for wireless LANs (WLANs) and has enjoyed a substantial increase in the number of individuals and businesses "turning on" Wi-Fi networks.

[0005] In fact, many businesses are beginning to offer wireless networking services to their employees and their customers. In most cases, the business pays for a broadband wired backhaul service or other network transport service that connects the business to a global communication network like the Internet and, then, the business makes that connection available to employees and customers across a wireless LAN.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The present invention is pointed out with particularity in the appended claims. However, features are described in the following detailed description in conjunction with the accompanying drawings in which:

[0007] FIG. 1 shows a block diagram of a network and data access system incorporating teachings of the present disclosure. The system of FIG. 1 depicts a private network operator with multiple wireless LAN hubs;

[0008] FIG. 2 depicts a simplified flow chart for a network and data services access method that incorporates teachings of the present disclosure; and

[0009] FIG. 3 depicts a communication system that incorporates teachings of the present disclosure. The system of FIG. 3 shows multiple web-based data services, multiple private network operators, and a federated access system.

DETAILED DESCRIPTION OF THE DRAWINGS

[0010] Wireless services often authenticate users based on the handset or the device associated with a given user. The wireless service provider usually recognizes and authenticates the associated device and, as such, the user, while the device is seeking access to the service provider's network. In many cases, the operator is both the identity provider and the service provider.

[0011] In the wireline Internet model, data service providers and network transport service providers may be different entities. In many cases, the step of network authentication may be implicit. An authenticated network connection may exist or be launched "behind the scenes" as a result of launching a web browser or other application. In practice, the user may only see the step of authenticating to individual data service providers.

[0012] The Wi-Fi service model may be a mix of the two. The user may authenticate with the network either implicitly (device-based) or explicitly (user-name/password). Because data services may be offered by any provider (following the general Internet model), there may be an additional need to authenticate with each of these service providers. Among other things, teachings in the present disclosure describe a technique for leveraging the fact that a user has already authenticated to the network and using this to also authenticate to services. In order to facilitate authentication to a network transport service and a wide range of service providers, an identity provider may vouch for the user's identity.

[0013] Identity, which may include related attributes like profile, location and presence, may facilitate enablement of a range of Wi-Fi services, like customized coupons as you enter a mall, directions to nearby restaurants, etc. There may be several ways to architect a system incorporating teachings of the present disclosure. In one embodiment, hotspot authentication by a local access controller may be passed along to other providers, effectively treating the access controller as a federated service provider.

[0014] In other embodiments, user authentication to the network may occur in multiple ways. A user may explicitly enter username and password to authenticate to the network. The process may use the MAC address associated with the device. A secure digital certificate stored on the device may be used. In addition, each of the device-based authentication schemes may further be augmented by username/password or biometrics; and/or the access controller may support the Radius authentication protocol. In this case, the access controller may pass the credentials to a Radius Proxy, which could communicate with an identity server using other protocols (like SAML, XML, etc). As mentioned above, the network authentication may be federated with the identity provider.

[0015] In one embodiment, network authentication may offer a basic level of service authentication, while access to services that require higher security would make the identity provider prompt the user for additional credentials. In some embodiments, the access controller and the identity provider may be the same entity. In this case, when the user is authenticated to the network, the user is simultaneously authenticated to the services registered with the identity provider. The teachings of this disclosure are described below with reference to specific embodiments.

[0016] As mentioned above, many businesses are beginning to offer wireless networking services to their employees and their customers. In a typical situation, the business pays for a broadband backhaul service or other network transport service that communicatively connects the business to a global communication network like the Internet. The business may then make the connection available to employees and customers using a wireless LAN. In some circumstances, the business may charge a fee for utilizing the business' transport service.

[0017] The fee may be prepaid, post-paid, and/or pay-per-use. The fee may based on some time-based metric like hourly, daily, or monthly. The fee may also be based on another unit of measure all together like bits across the network. In some prepayment embodiments, a user may enter a credit or debit card number. The user may also purchase a prepaid access card and provide information associated with that card to an entity providing transport and/or data services.

[0018] Whatever the basis for billing, the business will likely need to know who is accessing its network and utilizing its transport service. The business may want to track how long the user has been on-line, how much data the user is pushing, how to bill the user, and how the user plans to pay. Much of this information is easier to gather if the user is registered and required to "log-in" to the transport service.

[0019] Occasionally, the business will provide access to the transport service for free. In situations where the transport is offered for free, the business may still want and/or need to know who is on the business' network and who is accessing a larger network like the Internet through the business' wireless LAN. As a result, a business providing free access may still ask a user of the wireless LAN to register or to log in to let the business owner know that he or she is "connected" to the business' network and potentially through the business network to a broader network.

[0020] Whatever the motivation, businesses that make their transport services available to customers and employees via a wireless or wired LAN may want the individuals using the service to log-in with credentials that uniquely identify the individual. Unfortunately, this seemingly reasonable desire on the part of business owners may create yet another user name and password combination to be remembered. Moreover, once logged in to the transport service, a user may still need to log in to each data service to which the user belongs.

[0021] If the user has a web-based electronic mail account, the user may be prompted to enter another set of credentials. If the user has an on-line brokerage account, the user may be prompted to enter yet another set of credentials. As mentioned above in the brief description of the drawings, FIG. 1 shows a block diagram of a network and data access system 10 that incorporates teachings of the present disclosure. System 10 may help, among other things, alleviate some of the multi-step log-in difficulties discussed above.

[0022] As shown in FIG. 1, system 10 depicts a private network 12 with multiple wireless LAN hubs 14, 16, 18, and 20. Though the LAN hubs are depicted as wireless access points capable of wirelessly linking to computing devices, in some embodiments, a network operator may elect to connect hubs and computing devices with wires. In the

embodiment of FIG. 1, two wireless computing devices (laptop 22 and wireless phone 24) have short-range or local area wireless transceivers that serve to connect the devices to LAN hubs 16 and 18, respectively. Laptop 22 is "connected" to LAN hub 16 across wireless link 26, and wireless phone 24 is "connected" to LAN hub 18 across wireless link 28.

[0023] Laptop 22 and wireless phone 24 may each include several electronic components and computing devices. Both laptop 22 and phone 24 may also include a computer-readable medium having computer-readable data to initiate a query to find an 802.11 network, to initiate presentation of information that indicates at least one found network, to request connection to the at least one found network, to receive an input requesting retrieval of information associated with a network data service, to receive a request for user credentials, to initiate communication of input user credentials, and to maintain an authorization token indicating a right to access both the found network and the network data service.

[0024] Wireless links 26 and 28 may be the same type or different types of wireless links. The link type may depend on the electronic components associated with the given wireless devices and wireless LAN hubs. The wireless computing device and/or wireless hub (Wireless Enabled Devices) may include any of several different components. For example, a Wireless Enabled Device may have a wireless wide area transceiver, which may be part of a multi-device platform for communicating data using radio frequency (RF) technology across a large geographic area. This platform may be a GPRS, EDGE, or 3GSM platform, for example, and may include multiple integrated circuit (IC) devices or a single IC device.

[0025] A Wireless Enabled Device may also have a wireless local area transceiver as shown in FIG. 1, which may communicate using spread-spectrum radio waves in a 2.4 GHz range, 5 GHz range, or other suitable range. The wireless local area transceiver may be part of a multi-device or single device platform and may facilitate communication of data using low-power RF technology across a small geographic area. For example, if the wireless local area transceiver includes a Bluetooth transceiver, the transceiver may have

a communication range with an approximate radius of twenty-five to one hundred feet. If the wireless local area transceiver includes an 802.11(x) transceiver, such as an 802.11(a)(b) or (g), the transceiver may have a communication range with an approximate radius of one hundred fifty to one thousand feet.

[0026] As shown in FIG. 1, LAN hubs 14 and 16 make up part of wireless site 30, and LAN hubs 18 and 20 make up part of wireless site 32, which may be geographically removed or remote from wireless site 30. In an 802.11(x) embodiment, wireless site 30 may be referred to as a hotspot. Wireless sites 30 and 32 may also include respective access controllers 34 and 36. Though shown within the site, access controllers may be located in other locations or removed all together.

[0027] Wireless sites 30 and 32 may be communicatively coupled to a network bridge 38 capable of connecting the sites to a private network management server 40. The sites may be connected through an access controller, as depicted, through some other intermediary devices, or directly. Management server 40 may be capable of receiving and responding to requests for private network information, which may be located in local data store 42. Management server 40 may also act as a gateway to a broader network. As shown, management server 40 is communicatively coupled to Internet 44 via link 46.

[0028] In practice, the information communicated across link 46 may be compressed and/or encrypted prior to communication. The communication may be via a circuit-switched network like most wireline telephony networks, a frame-based network like Fibre Channel, or a packet-switched network that may communicate using TCP/IP packets like Internet 44. The physical medium making up at least a portion of link 46 may be coaxial cable, fiber, twisted pair, an air interface, other, or combination thereof. In some embodiments, link 46 may be a broadband connection facilitated by an xDSL modem, a cable modem, another 802.11x device, some other broadband wireless linking device, or combination thereof.

[0029] In a preferred embodiment of system 10, a user may seek to log into Internet 44 and data services associated therewith. The user may be operating laptop 22 and connect

to wireless LAN hub 16 via link 26. The user may then use a browser like Netscape or Internet Explorer to request access to a web-based data service. In some embodiments, this request will be identified and the user will be directed to a unified access operator 48. Operator 48 may be a company or service that manages subscriber credentials for a federation of private network operators. Operator 48 may provide authentication and access services to the LAN operators.

[0030] Though operator 48 is depicted as a remote authentication service bureau for a third party private network operator in FIG. 1, operator 48 may, in some embodiments, operate its own collection of wireless sites, act as an authentication service bureau for a plurality of third party network operators, provide transport services, provide web-based data services, or engage in any other activity.

[0031] Operator 48 may have a gateway 50 that receives an initial set of credentials from the requesting user attempting to access transport and data services from laptop 22. Gateway 50 may communicate with authentication engine 52, which may be capable of comparing the initial set of credentials against information maintained in data store 54. In some embodiments, gateway 50 may re-direct the requesting user to an identity provider, which may be a third party. The identity provider may authenticate then authenticate the requesting user.

[0032] If the credentials are verified, authentication engine 52 or a component of a third party identity provider may output an "accepted" signal, which may be directed to an authorization engine like authorization engine 56. In response to the accepted signal, authorization engine 56 may grant laptop 22 and its user access to both the transport services offered by the operator of private network 12 and the data services of federated web-based data service providers.

[0033] In some embodiments, operator 48 may provide data services like web-based electronic mail, voice mail accounts, a unified messaging service, financial account services, customized home page services with user-selected content presented in a user-defined format, some other user-specific data service, and/or combinations thereof. To offer these data services, operator 48 may employ a data service application server 58,

which may have a data store 60. In preferred embodiments, the access granted by authorization engine 56 will allow the user of laptop 22 to bypass any additional log in procedures that may have been otherwise necessary to access the data services of operator 48 or the data services of other federated data service providers.

[0034] Embodiments supporting simplified access to federated data service providers may make use of some security standards like WS-Security for high-level security services, XACML for access control, XCBF for describing biometrics data, SPML for exchanging provisioning information, and XrML for rights management. As deployed, system 10 may use at least one version of the Security Assertion Markup Language (SAML). SAML is an authentication language with an Extensible Markup Language (XML) based framework. SAML may help secure transmitted communications over local communication networks and broad communication networks like the Internet.

[0035] SAML may also be used to define federation exchange mechanisms that facilitate the exchange of authentication, authorization, and nonrepudiation information. The Organization for the Advancement of Structured Information Standards (OASIS) recently ratified Version 1.0 of SAML, which is incorporated herein by reference. In preferred embodiments, deployed systems incorporating teachings of the present disclosure may also include additional security enhancements, such as opt-in account linking, multiple levels of log in, simple session management, and global log-out capabilities.

[0036] For example, authorization engine 56 may require relatively low security credentials to access a unified mailbox and higher security credentials to access financial-based data services. Credentials may take several forms. Credentials may include, for example, device-based identifiers, machine readable identification information, username/password combinations, and/or biometric information like finger prints or retinal scans.

[0037] In operation of system 10, a component of operator 48's network may be a server made up of a microprocessor, a personal computer, a computer, some other computing device, or collection thereof. The server or servers may be operating as one or more of the above described engines in addition to other engines. The server or servers may also

include a computer-readable medium having computer-readable data to access maintained credentials of a plurality of users, to direct an authentication engine to compare input credentials against maintained credentials, to signal an authorization engine of accepted input credentials, and to initiate communication authorizing access to both a network transport service and a network data service.

[0038] An understanding of system 10's operation may be more readily understood by reference to FIG. 2. As mentioned above, FIG. 2 depicts a simplified flow chart for a network and data services access method 70 that incorporates teachings of the present disclosure. Method 70 imagines an embodiment similar to system 10 of FIG. 1 having multiple wireless access points. Method 70 may also be applied to wired LAN applications, and system 10 could make use of a method other than method 70.

[0039] As depicted in FIG. 2, method 70 begins at step 72 when a subscriber comes into range of a wireless access point. The user may search for available wireless networks using a sniffer application that identifies available access points. In preferred embodiments, the sniffer application may present the user with a displayed pick list of available LAN hubs and present an icon in connection with those hubs associated with a federated network.

[0040] The user may find a federated hub and link to it at step 74. At step 76, the user may use a browser to request some web-based content. For example, the user could type in a URL of a unified messaging home page. The user and/or the user's request may be recognized at step 78 by an access controller, which may be a software engine operating at a computing platform local to or closely connected to the access point. The software engine may also be operating at a remote location like gateway 50 of FIG. 1. At step 78, an access controller may provide a page to the user. The page may include information related to the location of the access point.

[0041] At step 80, a system incorporating method 70 may ask the subscriber if the subscriber desires broad or local network access. If the subscriber indicates at step 82 a desire for broad network access, method 70 may move to step 84 and the subscriber may be prompted to enter a first set of credentials. For example, the user may be prompted to

enter a user name and password combination. If the subscriber credentials are authenticated at step 86, the subscriber may be granted access to both federated data services and federated network transport services at step 88.

[0042] The federated transport services may be embodied by the wireless LAN access point the subscriber initially connected to at step 74 as well as the transport services connecting that access point to a broad global communications network like the Internet. The federated transport services may also include wireless and wired LANs operated by the same party operating the wireless LAN to which the subscriber is currently connected. The federated transport services could also include wireless and wired LANs operated by federated third parties or any other appropriate communication transport service.

[0043] In one embodiment, a system executing method 70 may lease a token to the subscriber at step 90, and the token may be cached on the computing device being used by the subscriber. As such, when the subscriber roams at step 92 to another federated transport service or browses to another federated web-based data service, the subscriber will be "recognized" and will not be asked to go through another credential exchanging log in.

[0044] In some embodiments, the subscriber may have linked several computing devices to his or her account. In such an embodiment, a token may be leased to each of the subscriber's linked devices – allowing the subscriber to connect with different devices at the same or different times. A system executing method 70 may limit this log in free connection period to some defined metric. The defined metric may be the length of time or the number of connections for which the token or tokens are leased.

[0045] If at step 82, the subscriber elects local log in, method 70 may move to step 94 where the subscriber keys in local log in information. Once the credentials are authenticated at step 96, the subscriber may be granted access at step 98 to locally stored information or some limited walled-garden list of information. Whether broad or local network access is requested, method 70 may eventually progress to a stop at step100.

[0046] An operator may want to provide both a broad and local network option to subscribers. In some cases, access to the broad network may be offered as a for-pay option and access to the local network may be offered for free or at a reduced rate. The local network may include location-specific information like a map of the area or a menu for a nearby restaurant.

[0047] As mentioned above, FIG. 3 depicts a communication system 102 that incorporates teachings of the present disclosure. System 102 depicts two private networks 104 and 106 connected to a global communication network like Internet 108, a unified access operator 110, and two web based data services 112 and 114. As depicted, private networks 104 and 106, access operator 110, and data services 112 and 114 are part of a federated network and share subscriber identity information, log in credentials, and log in state with one another across Internet 108.

[0048] In a preferred embodiment of system 102, a subscriber may register with access operator 110 as a federated subscriber. The federated subscriber may have identified a group of federated third party data service providers with whom the subscriber will "allow" access operator 110 to share credentials. If data services 112 and 114 are included in the subscriber's linking list, the subscriber may be able to log in once via access operator 110 and roam unencumbered between federated data services 112 and 114 and data services provided by access operator 110.

[0049] Similarly, if the subscriber selects a federated transport service provider, the act of logging in to the transport service may automatically log the user in to federated data services – effectively removing the obligation to log in again and again as the subscriber moves from third party site to third party site, without regard for whether the third party sites has a transport-focus or a web-based data-focus.

[0050] Though the process described above indicates that a user may log in via the access operator, in other embodiments, the log in may occur at another federated site. The process of sharing credentials and granting access to both transport and data services may be effectuated and/or initiated by entities other than access operator 110. As depicted in system 102, access operator 110 may act as a clearing house or a service bureau for other

entities, but other techniques may be employed without departing from the teachings of the present disclosure.

[0051] It will be apparent to those skilled in the art that the disclosed embodiments may be modified in numerous ways and may assume many embodiments other than the particular forms specifically set out and described herein.

[0052] Accordingly, the above disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments that fall within the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.